Mapleによる数学実験 : 楕円曲線での例など (数式処理と教育)

AUTHOR(S):

中島, 匠一

CITATION:

中島, 匠一. Mapleによる数学実験 : 楕円曲線での例など (数式処理と教育). 数理解析研究所講究録 2010, 1674: 5-11

ISSUE DATE:

2010-01

URL:

http://hdl.handle.net/2433/141221

数理解析研究所講究録
第1674巻 2010年 5-11

Mapleによる数学実験（楕円曲線での例など）

学習院大学・理学部・数学科　　中島 匠一 (Shoichi Nakajima)
Department of Mathematics,
Faculty of Science,
Gakushuin University

1　はじめに

筆者は、(大ざっぱなくくりで)「整数論」を専門としている数学の研究者で、教育方面では、理学部数学科の学生を教えることを主な仕事としている。近年の計算機ハードウェアの急速な高性能化に伴って、数学の研究・教育に数式処理ソフトを利用することが現実味を帯びてきた。実際に、数学の研究論文に提示される計算データも、従来は計算機の専門家と協力して専用のプログラムを作成していることが多かったが、最近は数学者である著者自身がMathematicaやMapleなどの汎用数式処理システムを利用していることが多い。つまり、決して計算速度が速いとはいえない数式処理システムでも、数学的知見を得るのに十分な実験データが得られるようになった、ということである。

この流れを受けて、筆者はここ数年にわたって数学の研究・教育にMapleを活用することに力を注いでいる。研究集会では、学部生に対する数学教育、および、大学院生と共同でおこなった数学研究におけるMapleの利用について「事例紹介」をおこなった。今回の報告は集会での発表原稿に基づいて作成したので、記述が「羅列的」になってしまっているが、この点はお許し願いたい。また、後半の大学院生の研究については、考察した問題と研究結果の概略だけをまとめたので、詳しい結果に興味のある方は、最後に参考文献として挙げた修士論文を参照していただきたい。

2　学習院大学でのMapleの利用

筆者の周辺でのMapleの利用環境は、現在次のようになっている。

ライセンス形態

- サイトライセンスが導入されている
- 平成１４年に大学、男子中高、女子中高の３キャンパスのライセンスを購入（当時はMaple8）
- 平成２１年より、学校法人としてのサイトライセンス契約（製造元であるmaplesoft社の方針変更）

- さらに、数学科では、学生ライセンスを購入してきた
- 平成２１年度より、学生ライセンスが無料となった

このような経緯を経て、現在、学生は大学構内のコンピューター および 自宅のコンピューターで、自由に Maple が利用できる。ただし、物理的にソフトが利用可能となっても、実際に学生が利用するに当たっては「使い方を覚えなくてはならない」というハードルがあり、このハードルの高さは無視できない。この困難に対処するために、数学科として、Maple の説明書を作成している。また、長年 Maple の日本総代理店であり現在は maplesoft 社の親会社となったサイバーネット社の技術者を招聘して、集中講義形式で Maple の指導をお願いしている（科目は、「数学講話 1」）。この講義は学生には好評である。

数学科での Maple の利用

(1) 4 年ゼミでの利用

・中島ゼミ・中野ゼミ（整数論）：

楕円曲線に関する計算（具体的には、因数分解のレンストラ法の実装および性能の実験、階数の高い楕円曲線の探索、楕円曲線を利用したイデアル類群の元の構成、など）。

・川崎ゼミ（幾何）：

各種の多面体の３Ｇ表示および模型作成。

（注：川崎教授は Mathematica 利用；Maple を利用することも可能。）

・水谷ゼミ（解析）：

偏微分方程式の数値解法。

(2) 講義での参考資料の作成

関数のグラフを見せる、アニメーション機能を利用してパラメーターが変化したときの様子を見せる、など。

(3) 学生の自主的な利用

練習問題の答えのチェック、グラフの描画、など。

「数学輪講」で、自主的なテーマの追及。

(4) 数学の研究への利用（中島の場合）

・中島ゼミの院生：

楕円曲線の $\mathbf{F}_p$ 有理点の群構造の研究に利用。

・中島自身の研究：

円分体の類数のパリティー

2次体の類数の mod m 剰余

結び目のアレキサンダー多項式

Euler-Kronecker 定数

…… 。

Mapleの利用のメリット

Mapleは安直な利用も可能であるが、本格的にプログラミングすることもできる。数学科では、基本的にプログラミングを実践している。

Mapleの教育上のメリットとして、次のことがあげられる。

(1) （論理性）「プログラム力＝論理力」といってもいいくらいで、実際、数学のできる人はプログラミングを覚えるのが早い。逆に、プログラム作成を通して論理性を身に付けていくことも可能である。

(2) （正確な理解）きちんと動くプログラムを書くには、数学的内容の正確な理解が求められる。本を読んだだけでは分からない論点に、プログラム作成を通して気づくこともある。

(3) （成功体験）どんな簡単なプログラムでも、自分で作ったものがちゃんと動くと嬉しいものである。成功体験は充実感につながり、数学を勉強し続ける原動力になり得る。

(4) （自主性）プログラムを書くこと自体にも自主性が必要であるし、テーマを自分で選ぶようになれば、自主性を発揮する領域は無限に広がる。学部生が新しい現象を発見することも不可能ではない。

最近の計算機の発展は目覚ましく、数式処理は「実用段階」に達している。実際に、MapleやMathematicaで計算したデータをもとに議論を進めている論文も多数登場している。我々のゼミでも、大学院生は全員Mapleを利用して「実験」を進めて、新しい事実の発見に成功している。

Mapleの利用上の問題点

Mapleに限らず、数式処理システムは数学に関わる計算ならどんなものでも高速に実行してくれて、とても楽しく面白いが、

利用にあたって、最初のハードルが高い

という難点があり、活用の妨げになっている。（基本的な利用法を覚えるのがなかなか大変。）

また、研究レベルで活用する場合には

高度な利用のためには、コンピューターの仕組みに関する知識が必要となる

という点も問題になってくる。

問題点への対策

上記の問題点について、以下のような対策を実施（および、考慮）している。

(1) 利用マニュアルを作成し、配付（Maple11 版；Maple12 でも通用)。

(2) 「数学輪講」（選択科目）で実習させる（大学院生が TA を勤めている)。

(3) 「数学講話」（選択科目）で講習をおこなう（以前は中島が担当、最近はサイバーネット社から講師を呼んでいる)。

(4) 現在 C 言語を教えている「計算機 I 、 II」（選択科目だが、準必修）の時間の一部で Maple を扱うことを検討中（現在、限定的に実施)。

(5) 学生の参考となるように、具体的な教材を作成する計画をたてている。今年度に学習院内部の予算が獲得できたので、微積分の教材を作成することが決まった。

3 Mapleを利用した、大学院生の研究

3 人の大学院生が、楕円曲線の整数論での研究をおこなった。そのテーマは、次のものである。

(1) 有理数体上の楕円曲線と素数 p に対する $(n_{1,p}, n_{2,p})$ の分布（記号は下記）
萩原　賢紀（平成１９年修了）
駿河　大輔（平成２０年修了）

(2) 楕円曲線の等分多項式
黒崎　麻衣（平成２０年修了）

3.1 楕円曲線に関する説明

楕円曲線 E とは、xy-平面内で

$$y^2 = x^3 + ax^2 + bx + c$$

という等式で定まる曲線のこと。

注１： a, b, c は定数で、3 次式 $x^3 + ax^2 + bx + c$ は重根をもたない、という条件を満たしている。

注２：正確には、射影平面で考えなければならない。

このとき、E の上には無限遠点 $\mathcal{O}$ が 1 つ存在する。

楕円曲線の群構造

楕円曲線の重要な性質として

楕円曲線上の点全体は可換群をなす

ということがある。これが、楕円曲線曲線の魅力の源泉である。

群構造の定まり方を簡単に述べると

・ゼロ元（群の単位元）は、無限遠点 $\mathcal{O}$

・一直線上にある3点の和はゼロに等しい
・Pの逆元は、x軸に関してPと対称な点である
となる。

$(n_{1,p}, n_{2,p})$の分布
楕円曲線

$$E : y^2 = x^3 + ax^2 + bx + c$$

を

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$$

上で考えることができる（pは素数)。
このとき、Eの$\mathbf{F}_p$有理点の集合$E(\mathbf{F}_p)$は

$$\{(x, y) \in \mathbf{F}_p^2 \mid y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathcal{O}\}$$

と表される。
楕円曲線に関する基礎理論によって、$E(\mathbf{F}_p)$について次のことが知られている。

FACT:　有限アーベル群として

$$E(\mathbf{F}_p) \cong \mathbf{Z}/n_{1,p}\mathbf{Z} \oplus \mathbf{Z}/n_{2,p}\mathbf{Z}$$

が成り立つような自然数$n_{1,p}, n_{2,p}$で

$$n_{1,p} \text{ は } n_{2,p} \text{ の約数}$$

をみたすようなものが唯1組定まる。ここで、自然数nに対して、$\mathbf{Z}/n\mathbf{Z}$は位数nの巡回群を表す。（つまり、$E(\mathbf{F}_p)$は高々2つの巡回群の直和となる。）

3.2　萩原の研究

a, b, cを整数として、楕円曲線

$$E : y^2 = x^3 + ax^2 + bx + c$$

を考える。このとき、素数pに対して「Eの、pを法とする還元(reduction)」を考えると

$$E(\mathbf{F}_p) \cong \mathbf{Z}/n_{1,p}\mathbf{Z} \oplus \mathbf{Z}/n_{2,p}\mathbf{Z}$$

をみたす自然数の組$(n_{1,p}, n_{2,p})$が定まる（上記の**FACT**参照)。

問題：素数pを動かすとき、$(n_{1,p}, n_{2,p})$の分布を調べよ。

1つの成果：$a = c = 0$の場合について、$n_{1,p}$の分布の法則を解明した。また、その結果をもとにして、CM型（つまり、虚数乗法をもつ）楕円曲線について$n_{1,p}$の分布を解明する道筋がわかった。

その他の成果：$\dfrac{n_{2,p}}{n_{1,p}}$についても、興味深い性質に気づいた。

3.3 駿河の研究

素数 p を 1 つ固定して、a, b, c を $\mathbf{F}_p$ の元とする。
このとき、d を法 p の平方非剰余として、楕円曲線

$$E : y^2 = x^3 + ax^2 + bx + c$$

のツイスト (twist)

$$E' : y^2 = x^3 + adx^2 + bd^2x + cd^3$$

を考える。
すると、E' についても

$$E'(\mathbf{F}_p) \cong \mathbf{Z}/n'_{1,p}\mathbf{Z} \oplus \mathbf{Z}/n'_{2,p}\mathbf{Z}$$

をみたす組 $(n'_{1,p}, n'_{2,p})$ が定まる。
注：E' は、楕円曲線として

$$dy^2 = x^3 + ax^2 + bx + c$$

に同型である。また、d を取り替えても、得られる E' の同型類は変わらない。

問題:素数 p を固定して、$\mathbf{F}_p$ 上の楕円曲線 E を動かす。このとき、$(n_{1,p}, n_{2,p})$ と $(n'_{1,p}, n'_{2,p})$ にはどんな関係があるか？

１つの成果：例外となる唯 1 つの曲線をのぞいて、積 $n_{1,p}n'_{1,p}$ に（非自明な）上界があるらしいことがわかった。ただし、例外の曲線（j-不変量が -15^3 の楕円曲線）が現れる理由は、いまのところ、全くわかっていない。

3.4 黒崎の研究

係数 a, b, c は任意の数として、楕円曲線

$$E : y^2 = x^3 + ax^2 + bx + c$$

を考える。
このとき E は可換群なので、自然数 n と E 上の点 P に対して、

$$P \text{ を } n \text{ 倍する（}nP \text{ を求める）}$$

という操作が考えられる。
この操作の結果を具体的に表すのが「等分多項式」である。
特に n が奇数のときには、

$$P = (x, y)$$

として

$$nP = \left(\frac{\phi_n(x)}{\psi_n(x)^2}, \frac{y\omega_n(x)}{\psi_n(x)^3} \right)$$

をみたす多項式 $\psi_n(x), \phi_n(x), \omega_n(x)$ が定まることがわかっている。

（n が偶数のときも同様である。しかし、記号が少しかわるため、具体形は省略する。）

等分多項式のみたす漸化式が昔から知られており、それによって帰納的に計算することができる。

漠然とした問題設定：等分多項式の「新しい性質」を見つけよ。

具体的（だが、特殊）な問題：

（1）等分多項式の、与えられた次数 k の係数を n, k, a, b, c を用いて表せ。

（2）a, b, c が整数のとき、等分多項式の content（＝係数すべての gcd）を決定せよ。

1つの成果：任意の n について、等分多項式の「最高次に近い次数の係数」と「最低次（定数項）に近い次数の係数」は決定できた。また、その応用として、かなりの場合に、content の決定もできた。さらに、新たな観察として、$c = 0$ の場合に係数が簡単になることが多いことがわかった。これは、従来の計算では明確になっていなかった事実である。

3.5 Maple利用に関するコメント

萩原・駿河の研究は、一応、「数値計算」範囲である。

この場合の Maple のメリットは、

(1) 任意の（多倍長の）整数演算が自由におこなえる

(2) 代数的な数（特に、有理数）について近似計算でなく厳密計算が可能

という点である。

黒崎の研究には、非常に高い次数の多項式が登場するが、これらの多項式の計算は膨大で、手計算ではほぼ不可能である。多項式の計算を手軽におこなってくれる数式処理システムを利用できたことの意義は非常に大きい。

参考文献

[1] 萩原賢紀，楕円曲線の $\mathbf{F}_p$ 有理点の群構造の分布，学習院大学大学院自然科学研究科（数学専攻）修士論文, 平成 19 年度.

[2] 黒崎麻衣，楕円曲線の等分多項式の係数について，学習院大学大学院自然科学研究科（数学専攻）修士論文, 平成 20 年度.

[3] 駿河大輔，$\mathbf{F}_p$ 上の楕円曲線とその twist の群構造，学習院大学大学院自然科学研究科（数学専攻）修士論文, 平成 20 年度.